NISSC - Oct 96

Workshop Report on
The Role of Optical Systems and Devices for Security

Security for All-Optical Networks

Jeff Ingle
R22
National Security Agency
9800 Savage Rd., Suite 6516
Ft. Meade, MD 20755-6516

jtingle@alpha.ncsc.mil
301-688-0291 ph
301-688-0289 fax

Scott McNown
R22
National Security Agency
9800 Savage Rd., Suite 6516
Ft. Meade, MD 20755-6516

srmcnow@alpha.ncsc.mil
301-688-0291 ph
301-688-0289 fax

Vision of Emerging All-Optical Networks

Motivation

- **Drive for more bandwidth - will push aggregate rates of ATM/SONET past highest defined OC-192 (9.6 Gbps)**
- **Need to protect information - both information security (INFOSEC) and survivability**
- **INFOSEC (security mechanisms) and Survivability (counter vulnerabilities) share solutions**
- **Opportunities to incorporate INFOSEC and survivability into emerging networks and standards**

Vision of Emerging All-Optical Networks

Emerging All-Optical Networks

- **Near-term technology**
  - **Time Division Multiplexing (TDM) combined with Wavelength Division Multiplexing (WDM)**
  - **Probably multiple OC-192 (9.6 Gbps TDM) channels, on multiple wavelengths (WDM)**
- **Circuit-switched all-optical networks**
- **Packet-switched all-optical networks**
- **Longer-term technologies**
  - **Solitons, CDMA, Quantum communications, Wideband coherent comm.**

Research approach for security and survivability

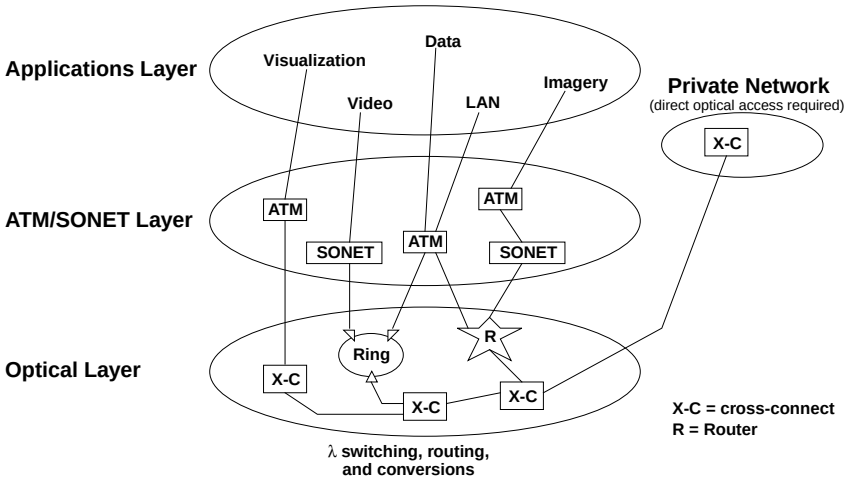
Network Architecture Study

- **Vulnerabilities and Countermeasures**
- **Security in Network Management**
- **Hooks for other security and survivability**

Research to develop devices and components

- **To incorporate countermeasures in vulnerable components**
- **To provide security mechanisms like confidentiality (encryptors)**

Circuit-switched all-optical network topology



Circuit-switched optical networks

Network Architecture Study

Architecture
- topology, network node composition, service provisioning and signaling
- security implications of "just-in-time" signaling for minimal latency

Network Control and Management (NC&M)
- fault detection and localization, configuration management, quality of service (QoS) management, security management, resource allocation

Authentication
- of end users, signaling, QoS negotiation
- for access control, accounting and billing

Security service negotiation capability
- level of security, type of encryption and key exchange algorithm, authentication protocol, data integrity, etc. (possible model in IPv6)

Research to develop devices and components

Survivability of common optical network components
- Optical multiplexers, optical routers, optical amplifiers
- Reduce vulnerability to jamming, reduce crosstalk, organize subsystems within component for best resistance
- Develop - comprehensive set of design rules, methods to counter attacks, robust devices

Confidentiality and key management
- Use symmetric encryption algorithms (e.g. DES) for high speed encryption, public key cryptography to distribute keys (although slow)
- Extend SONET encryptor model to WDM environment
- Need for optical encryptors is niche market - DoD, DOE, NASA supercomputing facilities

Network Security Managers

Packet-switched optical networks

Difficult challenge - emerging architectural possibilities

Network Architecture Study

- Follow similar approach as for circuit-switched optical networks
  - Authenticated signaling, flexible security negotiation mechanisms, security fields in signaling for crypto sync/resync - especially when no initial end-to-end connectivity

Research to develop devices and components

- Counter vulnerabilities in network components like switches or routers
- Optical packet encryptor
  - Word-based - one-dimensional string of bytes
  - Page-based - two-dimensional array of bytes
  - Need packet identifier, key generator (KG), optical delay, optical XOR

Longer-term technologies

Soliton transmission technology
- near term implementation in intercontinental submarine links
- could emerge as long term network technology
- confidentiality - mux parallel encryptors or high-speed cryptographic algorithm in technology like fiber loop logic

Code Division Multiple Access (CDMA)
- optical spread spectrum techniques
- privacy system, limited in distance and networking
- may be possible to use very fast cryptographic algorithm and technology to implement for high security

Quantum Communications

Quantum Cryptography
- high security (not based on public key techniques like factoring)
- limited bandwidth and distance - cannot network
- might be used for key distribution

- may reduce threat of covert channels
- may not be feasible in network situation

Wideband coherent communications
- may reduce threat of covert channels
- may not be feasible in network situation